POLICY SUMMARY OF THE PROPOSED IDENTITY MANAGEMENT LIABILITY LEGISLATION FOR VIRGINIA – JCOTS IDENTITY MANAGEMENT ADVISORY COMMITTEE (September 2014)

Prepared by CertiPath, Inc., Reston, Virginia

Growing the Digital Identity Market – Overcoming the Legal Barriers

There is a lot of talk about enabling federated identity management in cyberspace – the creation of a virtual identity credential that does for cyberspace encounters what the driver's license does for physical encounters. The goal is a marketplace providing a user-centric identity and authentication process that maximizes the ability of individuals to exercise informational privacy and access rights in the digital economy and e-government. However, whenever the discussion of a federated identity management in cyberspace marketplace is engaged, the topic very quickly comes round to liability. As the National Strategy for Trusted Identities in Cyberspace (NSTIC) puts it, "Uncertainty regarding the allocation and level of liability for fraud and other failures" is one of two identified significant barriers to the development of an identity management marketplace in the United States.

In particular, usage of identity credentials across sectors and communities of interest, both public and private, presents challenges not shared by the current bilateral identity credential scenario, where both parties are bound by contract concerning the distribution of liability. Like the credit card industry, the federated identity credential has unlimited relying parties; but unlike the credit card industry, these relying parties have no direct contractual relationship with the identity service providers to underpin liability risk allocations. In the absence of a contractual relationship or a statutory framework, the identity management marketplace is uncertain as to how courts will allocate liability.

The proposed legislation under consideration by the Virginia Joint Commission on Technology and Science (JCOTS) seeks to alleviate this uncertainty and create a legal framework for the identity industry along the lines of that which is afforded the credit card industry. It is not designed to remove liability, but to make liability manageable through codification in policy and procedural documentation made public by the identity provider.

A Legislative Solution to Promote the Emergence of a Digital Identity Industry – Establishing a Common Legal Foundation and Predictable Liability

The proposed legislation sets common operational and legal requirements for federated identity; thus providing a legal foundation for trust frameworks and the use of trustmarks as emerging approaches to implementing user-centric identity in the digital economy. In doing so, it adds a new Article to Chapter 3 of Title 8.01, comprised of three sections: 8.01-227.11 through 8.01-227.13.

Section 8.01-227.11 defines the set of applicable identity management terms associated with this legislation. In doing so, it sets in law these definitions and provides a basis for common interpretation.

Section 8.01-227.12 limits the applicability of the trustmark and leaves the provision of a warranty to the discretion of the identity provider.

Trust frameworks are an effective and flexible source of information policy rules with respect to implementing digital identity for the private and public sectors. A trustmark is associated with a

specific trust framework and signifies compliance with the trust framework's policies and procedures. As such, the trustmark is granted to identity providers and identity attribute providers that have undergone a specified certification process. The scope of such a trustmark is limited to the processes for determining identity. It does not extend to the integrity or trustworthiness of the individual to whom the identity credential has been provided or his or her behavior when involved in an electronic transaction. Therefore the proposed legislation specifically states that "use of a trustmark in a transaction does not imply a warranty for accuracy of the underlying informational content involved in the transaction." (Section 8.01-227.12.)

There are several trust frameworks already in use in Virginia, but undefined in statutes:

1) ConnectVirginia (DURSA and ONC);
2) Public universities (InCommon); and
3) The Cross Sector Digital Identity Initiative (AAMVA and VA DMV)

This legislation provides the underpinning for these trust frameworks to be recognized and protected under Virginia law.

Section 8.01-227.13 limits the liability of approved trust framework and identity providers to gross negligence or willful misconduct.

Even the most diligent identity verification process may be undermined by an individual intent on wrong-doing. The identity management marketplace needs to understand its liability if a digital identity credential is issued to an individual claiming an identity under false pretenses. To this end, the legislation provides the identity provider immunity from suit "unless the identity provider was grossly negligent or engaged in willful misconduct." (Section 8.01-227.13 B.)

On the public sector side, the Identity Advisory Committee has revealed the need for the Commonwealth of Virginia to designate an agency as the lead for the creation of a consistent identity policy for the citizenry in the provisioning of e-government services. The legislation will designate the Virginia DMV as the most logical and suitable agency to lead identity policy for the Commonwealth. To that end this legislation indicates that "trust framework providers (and identity providers) shall be immune from suit arising from any acts or omissions . . . that the Commissioner of the Department of Motor Vehicles for the Commonwealth of Virginia has deemed acceptable." (Section 8.01-227.13 A and B.)

Enabling the development of identity-related information policy rules through trust frameworks and trustmarks has several advantages over a traditional regulatory approach: 1) it avoids cross jurisdictional authority and choice of law challenges, 2) it provides greater flexibility and customization to suit the particular network and participant situations, and 3) it is easier to enforce against rule violators.

What this Could Mean for Virginia

Because of the critical mass of Virginia-based technology and its proximity to the Federal government, Virginia stands at the cross-roads of major industry developments in identity management. Proponents of this legislative effort believe that it will provide the needed catalyst for Virginia to become the center of a flourishing federated identity credentialing marketplace. This legal framework limiting the liability of

trust framework providers and digital identity credential providers will allow companies to facilitate identity credentialing platforms in Virginia and deploy those programs to their customer base throughout the U. S. with predictable liability risk protections under Virginia law.